EAT Update

Laurence Lundblade

IETF 114 July 2022

Important changes in the -13 and -14 drafts (since IETF 113)

- Document Organization
  - Claims section divided into 4: nonce, claims about entity, claims about token, cryptographic keys
  - Moved several sections to appendices; core of document is shorter now
- Specification changes
  - Use CoAP for content type of manifest and swevidence claims rather than CBOR tags
  - Added SPDX and CycloneDX manifest types
  - Measurment results claim reworked
  - Added a standard EAT CBOR profile for constrained devices.
- CDDL Improvements
  - Claims-Set now replicated in the document
  - No definition of UCCS, CDDL socket for where UCCS plugs in
  - Lots of improvements CDDL; validating for JSON and CBOR examples
- Lots and lots of wording improvements
  - Profiles section
  - Resynch with RATS Architecture terminology
  - For the following claims: UEID, SUEID, DLOAs Boot Count, cti & jti, nonce, SW Name,
  - Relation of Evidence to Attestation Results

Work in the EAT queue

- Security Considerations – some improvements needed
- Introduction and Abstract – some comments to address
- Varous other comments to address – mostly clarifications and small inconsistencies

- Possible minor improvements:
  - Optional nonce? – accommodate timestamp-based freshness in RATS architecture?
  - Add standard profile for JSON? – we have one for CBOR now